



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/054,027	01/22/2002	Jean-Philippe Champagne	CIS01-35(4747)	1449

7590 11/22/2005

Barry W. Chapin, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

EXAMINER

BAUM, RONALD

ART UNIT PAPER NUMBER

2136

DATE MAILED: 11/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/054,027	Applicant(s) CHAMPAGNE, JEAN-PHILIPPE	
	Examiner Ronald Baum	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____ | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

1. Claims 1-34 are pending for examination.
2. Claims 1-34 remain rejected.

Specification

The disclosure is objected to because of the following informalities: page 6, lines 10-13 are missing specific "U.S. Serial No." and filing date information.

Appropriate correction is required.

Claim 11 is objected to because of the following informalities: the phrase "... first request upon begin received by the server ..." is assumed to be "... first request upon being received by the server ...". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Liao et al, U.S. Patent 6,606,663 B1.

4. As per claim 1; "In a data communications device, a method providing authentication of a client device to a server device, the method comprising the steps of:

detecting a requirement for authentication of a request for data sent from

a client device to a server device [Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the limited capability client (i.e., '... the set of wireless client devices that wish to access protected resources ... network ...') for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

creating an authentication response in response to the step of detecting the requirement for authentication, the authentication response containing

authentication information required by the server device to allow

the client device to access data via the server device [Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

inserting the authentication response into the data communications session between

the client device and the server device,

the authentication response authenticating, to the server device,

access to the data by the client device [Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

~~maintaining the data communications session between~~

the server device and the client device

in the presence of authentication response information inserted into the data communications session between

the client device and the server device [Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].”.

Art Unit: 2136

As per claim 17, this claim is the apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; "A data communications device comprising:

at least one communications interface;

a memory;

a processor; and

an interconnection mechanism coupling the at least one communications interface, the memory and the processor;

wherein the memory is encoded with an authentication manager application that when performed on the processor, produces an authentication manager process that causes the data communications device to provide authentication of a client device to a server device by performing the operations of:

detecting a requirement for authentication of a request for data sent from
a client device to a server device;

creating an authentication response in response to the step of detecting the
requirement for authentication, the authentication response containing

authentication information required by the server device to allow
the client device to access data via the server device;

inserting the authentication response into the data communications session
between

the client device and the server device on the at least one communications
interface,

the authentication response authenticating, to the server device,
access to the data by the client device;
maintaining the data communications session between
the server device and the client device
in the presence of authentication response information inserted into
the data communications session between
the client device and the server device.”.

As per claim 33, ~~this claim is the embodied software claim for the method claim 1 above,~~
and is rejected for the same reasons provided for the claim 1 rejection, as such; “A computer
program product having a computer-readable medium including computer program logic
encoded thereon that, when performed on a computer system having a coupling of a memory, a
processor, and at least one communications interface, provides a method for authenticating a
client device to a server device by performing the operations of:

detecting a requirement for authentication of a request for data sent from
a client device to a server device;
creating, on the processor, an authentication response in memory in response to the step
of detecting the requirement for authentication, the authentication response containing
authentication information required by the server device to allow
the client device to access data via the server device;
inserting the authentication response into the data communications session between

the client device and the server device on the at least one communications interface,

the authentication response authenticating, to the server device,

access to the data by the client device;

maintaining the data communications session between

the server device and the client device

in the presence of authentication response information inserted into the data communications session between

the client device and the server device.”.

As per claim 34, this claim is the means plus function claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, as such; “A data communications device comprising:

at least one communications interface;

a memory; a processor; and

an interconnection mechanism coupling the at least one communications interface, the memory and the processor;

wherein the memory is encoded with an authentication manager application that when performed on the processor, produces an authentication manager process that causes the data communications device to provide authentication of a client device to a server device by providing a means including:

means for detecting a requirement for authentication of a request for data sent from a client device to a server device;

means for creating an authentication response in response to the step of detecting the requirement for authentication, the authentication response containing authentication information required by the server device to allow the client device to access data via the server device;

means for inserting the authentication response into the data communications session between the client device and the server device on the at least one communications interface, the authentication response authenticating, to the server device, access to the data by the client device;

means for maintaining the data communications session between the server device and the client device in the presence of authentication response information inserted into the data communications session between the client device and the server device.”.

5. Claim 2 *additionally recites* the limitation that; “The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises the step of:

detecting, in a data communications session between a client device and a server device,
an authentication request sent from the server device to the client device for
authentication of the client device by the server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the

Art Unit: 2136

proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 18, this claim is the apparatus claim for the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection, as such; "The data communications device of claim 17 wherein when the authentication manager process ~~causes the~~ data communications device to perform the step of

detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform the step of:

detecting, in a data communications session between a client device and a server device passing through the at least one communications interface,

an authentication request sent from the server device to the client device

for

authentication of the client device by the server device."

6. Claim 3 *additionally recites* the limitation that; "The method of claim 2 wherein the step of detecting an authentication request comprises the step of:

intercepting an unauthorized response sent from

the server device to the client device over the data communications session, the unauthorized response indicating that

the server device requires authentication of the client device in order for the client device to access the data using the server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) ~~are managed by the said intermediary processing element (i.e., col. 2, lines 45-64)~~, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 19, this claim is the apparatus claim for the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection, as such; “The data communications device of claim 18 wherein when the authentication manager process causes the data communications device to perform the step of detecting an authentication request, the authentication manager process causes the data communications device to perform the step of:

intercepting, on the at least one communications interface, an unauthorized response sent from

the server device to the client device over the data communications session, the unauthorized response indicating that

the server device requires authentication of the client device in order for

the client device to access the data using the server device.”.

7. Claim 4 ***additionally recites*** the limitation that; “The method of claim 3 wherein the unauthorized response from the server device is generated by the server device in response to an unauthenticated request for data sent from the client device to the server device over the data communications session.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 20, this claim is the apparatus claim for the method claim 4 above, and is rejected for the same reasons provided for the claim 4 rejection, as such; “The data communications device of claim 19 wherein the unauthorized response from the server device is generated by the server device in response to an unauthenticated request for data sent from

the client device to the server device over the data communications session.”.

8. Claim 5 *additionally recites* the limitation that; “The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises the steps of:

detecting, in a data communications session between a client device and a server device,
a request for data sent from a client device to a server device for access to data
using the server device;
caching the request for data in the data communications device; and
detecting, in the data communications session between a client device and a server
device,
an authentication request sent from the server device to the client device for
authentication of the request for data sent from
the client device to the server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 21, this claim is the apparatus claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection, as such; “The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform the step of:

detecting, in a data communications session between a client device and a server device,

~~a request for data sent from a client device to a server device for access to data~~
using the server device;

caching the request for data in the data communications device; and

detecting, in the data communications session between a client device and a server device,

an authentication request sent from the server device to the client device for

authentication of the request for data sent from

the client device to the server device.”.

9. Claim 6 ***additionally recites*** the limitation that; “The method of claim 1 wherein the step of creating an authentication response comprises the steps of:

obtaining authentication information associated with the client device, the authentication information capable of

authorizing, on behalf of the client device, access to the data using the server device; and
incorporating the authentication information into the authentication response such that the authentication response, when received by the server device due to the step of inserting,
allows the server device to authenticate access, by the client device, to data using the server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 22, this claim is the apparatus claim for the method claim 6 above, and is rejected for the same reasons provided for the claim 6 rejection, as such; “The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of creating an authentication response, the authentication manager process causes the data communications device to perform the step of:
obtaining authentication information associated with the client device, the authentication information capable of

authorizing, on behalf of the client device, access to the data using the server device; and
incorporating the authentication information into the authentication response such that the authentication response, when received by the server device due to the step of inserting,
allows the server device to authenticate access, by the client device, to data using the server device.”.

10. Claim 7 ***additionally recites*** the limitation that; “The method of claim 6 ~~wherein~~:

the authentication information is access control information; and wherein the step of incorporating comprises the steps of:

placing the access control information into
an authentication header of a packet of data serving as the authentication response to
allow the client device to access restricted data using the server device;
adjusting connection information associated with the packet of data to
account for the authentication information incorporated into
the authentication response; and
formatting the authentication response to
appear as though it originated from the client device.”.

Art Unit: 2136

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 23, this claim is the apparatus claim for the method claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection, as such; "The data communications device of claim 22 wherein; the authentication information is access control information; and wherein when the authentication manager process causes the data communications device to perform the step of incorporating, the authentication manager process causes the data communications device to perform the steps of:

placing the access control information into

an authentication header of a packet of data serving as the authentication response to

allow the client device to access restricted data using the server device;

adjusting connection information associated with the packet of data to

account for the authentication information incorporated into

the authentication response; and

formatting the authentication response to

appear as though it originated from the client device.”.

11. Claim 8 *additionally recites* the limitation that; “The method of claim 1 wherein:

the authentication response

is a packet including

an authentication header containing the authentication information and

is created by the data communications device to

~~appear as though it originated from the client device;~~ and wherein

the step of inserting the authentication response into the data communications session

between the client device and the server device comprises the step of

forwarding the authentication response to the server device over the data

communication session as at least one packet of extra data,

the authentication response being formatted to

appear as though it originated from the client device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 24, this claim is the apparatus claim for the method claim 8 above, and is rejected for the same reasons provided for the claim 8 rejection, as such; “The data communications device of claim 17 wherein;

the authentication response

is a packet including

an authentication header containing the authentication information and

is created by the data communications device to

appear as though it originated from the ~~client device~~; and wherein

when the authentication manager process causes the data communications device to perform the step of inserting the authentication response into the data communications session between the client device and the server device, wherein when the authentication manager process causes the data communications device to perform the step of

forwarding the authentication response to the server device over the data communication session as at least one packet of extra data,

the authentication response being formatted to

appear as though it originated from the client device.”.

12. Claim 9 *additionally recites* the limitation that; “The method claim 1 wherein the steps of detecting, creating, inserting and maintaining

are performed by the data communications device

without assistance from the client device and

are performed such that the data communications session between the client device and the server device

is free from disruption due to

authentication requirements of the client device to the server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 25, this claim is the apparatus claim for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection, as such; “The data communications device claim 17 wherein the steps of detecting, creating, inserting and maintaining

are performed by the data communications device

without assistance from the client device and

are performed such that the data communications session between the client device and the server device

is free from disruption due to

authentication requirements of the client device to the server device.”.

13. Claim 10 *additionally recites* the limitation that; “The method of claim 1 wherein the step of maintaining the data communications session between the server device and the client device after inserting the authentication response into the data communications session comprises the steps of:

maintaining connection state data in the data communications device that

tracks an amount of extra data associated with the authentication response that

is inserted into the data communications session

~~between the client device and the server device;~~ and

modifying connection information within packets passing through

the data communications device that are exchanged

between the client device and server device using the data

communications session in order to

allow the client and server device to maintain proper respective

first and second connection states for the data communications session

regardless of

the amount of extra data added in the data communications

session due to

insertion of the authentication response.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1,lines 13-col. 2,line 64, col. 6,lines 61-col. 8,line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server

Art Unit: 2136

(i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 26, this claim is the apparatus claim for the method claim 10 above, and is rejected for the same reasons provided for the claim 10 rejection, as such; “The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of maintaining the data communications session between the server device and the client device after inserting the authentication response into the data communications session, the authentication manager process causes the data communications device to perform the steps of:

maintaining connection state data in the data communications device that

tracks an amount of extra data associated with the authentication response that

is inserted into the data communications session

between the client device and the server device; and

modifying connection information within packets passing through

the data communications device that are exchanged

between the client device and server device using the data

communications session in order to

allow the client and server device to maintain proper respective
first and second connection states for the data communications session
regardless of

the amount of extra data added in the data communications
session due to

insertion of the authentication response.”.

14. Claim 11 ***additionally recites*** the limitation that; “The method of claim 1 wherein:

the steps of ~~detecting, creating, inserting and maintaining are repeated for at least a first~~
and second iteration; and

wherein for the first iteration:

the step of detecting a requirement for authentication of a request for data
comprises the step of

detecting an authentication request sent over the data communications
session from the server device to the client device in response to

the client device providing a first request for access to data using
the server device; and

wherein for the first iteration, the step of creating an authentication response
comprises the steps of

recreating the first request for access to first data and

placing authentication information into the recreated first request to allow

the server device to authenticate the recreated first request upon

begin received by the server device in the step of
inserting.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 27, this claim is the apparatus claim for the method claim 11 above, and is rejected for the same reasons provided for the claim 11 rejection, as such; “The data communications device of claim 17 wherein:

the authentication manager causes the data communications device to repeat the steps of detecting, creating, inserting and maintaining for at least a first and second iteration; and wherein for the first iteration:

when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data, the authentication manager process causes the data communications device to perform the step of

detecting an authentication request sent over the data communications session from the server device to the client device in response to

the client device providing a first request for access to data using
the server device; and
wherein for the first iteration, when the authentication manager process causes the
data communications device to perform the step of creating an authentication response,
the authentication manager process causes the data communications device to perform
the steps of
recreating the first request for access to first data and
placing authentication information into the recreated first request to allow
the server device to authenticate the recreated ~~first request~~ upon
begin received by the server device in the step of
inserting.”.

15. Claim 12 *additionally recites* the limitation that; “The method of claim 11 wherein, for
the second iteration of the steps of detecting, creating, inserting and maintaining:

the step of detecting a requirement for authentication of a request for data comprises
the step of detecting a second request for
access to data sent from the client device to the server device; and
wherein for the second iteration, the step of creating an authentication response
comprises the steps of:

intercepting the second request for access to data; and
generating an authentication response by

inserting the authentication information as an authentication header into
the second request to
allow the server device to
authenticate the second request for data on behalf of the
client device without requiring
generation of an authentication request; and
wherein for the second iteration, the step of inserting the authentication response into the
data communications session between the client device and the server device comprises the step
of:
forwarding the second request containing the authentication header to
the server device such that the server device can
authenticate the second request.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 28, this claim is the apparatus claim for the method claim 12 above, and is rejected for the same reasons provided for the claim 12 rejection, as such; “The data

Art Unit: 2136

communications device of claim 27 wherein, for the second iteration of the steps of detecting, creating, inserting and maintaining:

when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data, the authentication manager process causes the data communications device to perform

the step of detecting a second request for

access to data sent from the client device to the server device; and

wherein for the second iteration, when the authentication manager process causes the data communications device to perform the step of creating an authentication response, the authentication manager process causes the data communications device to perform the steps of:

intercepting the second request for access to data; and

generating an authentication response by

inserting the authentication information as an authentication header into the second request to

allow the server device to

authenticate the second request for data on behalf of the

client device without requiring

generation of an authentication request; and

wherein for the second iteration, the authentication manager process causes the data communications device to perform the step of inserting the authentication response into the data communications session between the client device and the server device, the authentication manager process causes the data communications device to perform the step of:

forwarding the second request containing the authentication header to
the server device such that the server device can
authenticate the second request.”.

16. Claim 13 *additionally recites* the limitation that; “The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises at least one of the steps of:

- a) detecting an authentication request being transmitted from
~~a server device through the data communications device to a client device in~~
response to the client device providing
a first request for data to the server device that requires authentication by
the server device; and
- b) detecting a second request for data being transmitted
through the data communications device from
the client device to the server device and
detecting that the client device provided
a first request for data to the same server device.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col.

Art Unit: 2136

2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 29, this claim is the apparatus claim for the method claim 13 above, and is rejected for the same reasons provided for the claim 13 rejection, as such; "The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform at least one of the steps of:

- a) detecting an authentication request being transmitted from
 - a server device through the data communications device to a client device in response to the client device providing
 - a first request for data to the server device that requires authentication by the server device; and
- b) detecting a second request for data being transmitted
 - through the data communications device from
 - the client device to the server device and
 - detecting that the client device provided
 - a first request for data to the same server device."

17. Claim 14 *additionally recites* the limitation that; "The method of claim 1 wherein: the data communications session is a transmission control protocol session between

the client device and the server device; and
wherein the step of maintaining modifies connection information within messages
exchanged between

the client device and the service device to account for the insertion of
authentication information inserted into the data communications session in order to
provide automatic authentication of requests for data sent to
the server device on behalf of client devices.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64; col. 6, lines 61-col. 8, line 23, ~~whereas~~ the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 30, this claim is the apparatus claim for the method claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection, as such; “The data communications device of claim 17 wherein:

the data communications session is a transmission control protocol session between
the client device and the server device; and

wherein when the authentication manager process causes the data communications device to perform the step of maintaining, the data communications device modifies connection information within messages exchanged between

the client device and the service device over the at least one communications interface to account for the insertion of authentication information inserted into the data communications session in order to

provide automatic authentication of requests for data sent to
the server device on behalf of client devices.”.

18. Claim 15 *additionally recites* the limitation that; “The method of claim 1 wherein the steps of detecting, creating, inserting and maintaining are
performed on behalf of a plurality of client devices and
wherein the authentication information is selected in the step of creating from different sets of authentication information based on at least one of
an address of the client device,
an address of the server device,
a type of data specified in the request, and
a protocol used to provide the request.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials

(i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), inclusive of the credential caching and request/response reformatting aspects, clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 31, this claim is the apparatus claim for the method claim 15 above, and is rejected for the same reasons provided for the claim 15 rejection, as such; “The data communications device of claim 17 wherein the steps of detecting, creating, inserting and maintaining are

performed on behalf of a plurality of client devices using
the same authentication information, and

wherein the authentication information is selected from different sets of authentication information based on at least one of

- an address of the client device,
- an address of the server device,
- a type of data specified in the request, and
- a protocol used to provide the request.”.

19. Claim 16 ***additionally recites*** the limitation that; “The method of claim 1 wherein the data communications device is

a device operating in a network to which hypertext transport protocol traffic is redirected to perform the steps of
detecting,

creating,
inserting and
maintaining.”.

The teachings of Liao et al suggest such limitations (i.e., Abstract, figures 1-3 and associated descriptions, col. 1, lines 13-col. 2, line 64, col. 6, lines 61-col. 8, line 23, whereas the use of the proxy server to act as the intermediary for the authentication of the client for associated server (i.e., WEB resources) via RFC2068 standards protocol resource access, whereas the credentials (i.e., user ID/password) are managed by the said intermediary processing element (i.e., col. 2, lines 45-64), ~~inclusive of the credential caching and request/response reformatting aspects,~~ clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

As per claim 32, this claim is the apparatus claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection, as such; “The data communications device of claim 17 wherein the data communications device is

a device operating in a network to which hypertext transport protocol traffic is redirected to perform the steps of

detecting,
creating,
inserting and
maintaining.”.

Art Unit: 2136

Conclusion

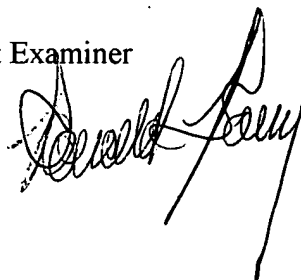
20. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be ~~obtained~~ from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100